

what it is

| | |
|-------------------------------------|----|
| why won't they listen? | 4 |
| simplex locks: illusion of security | 6 |
| dutch hacker intrusion | 14 |
| protecting your ssn | 18 |
| cocot numbers | 22 |
| letters | 24 |
| tidbits | 31 |
| postal hacking | 32 |
| psychology in the hacker world | 38 |
| 2600 marketplace | 41 |
| another dialer converted | 43 |
| useful unix programs | 44 |

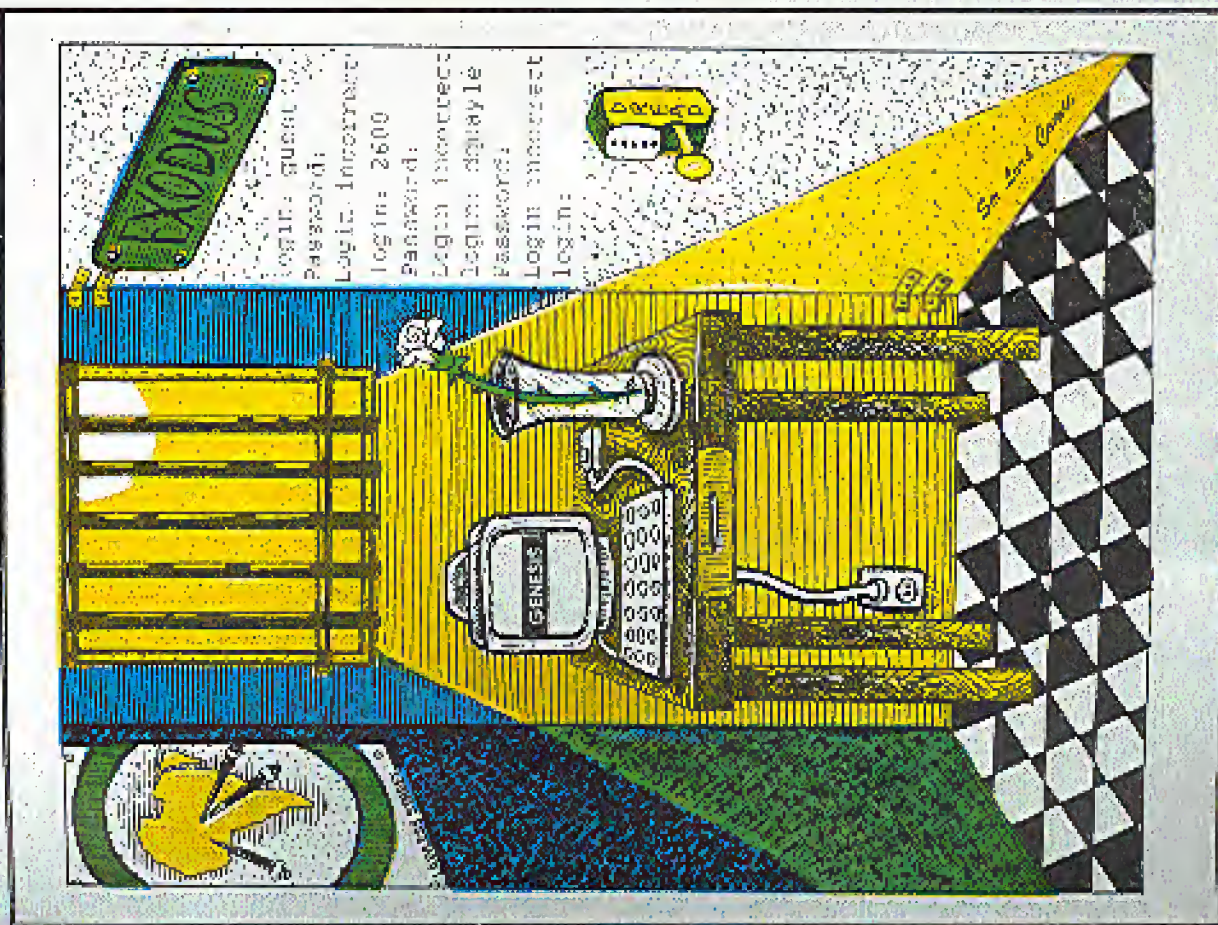
2600 Magazine
 P.O. Box 752
 Middle Island, NY 11953 U.S.A.
 Forwarding and Address Correction Requested

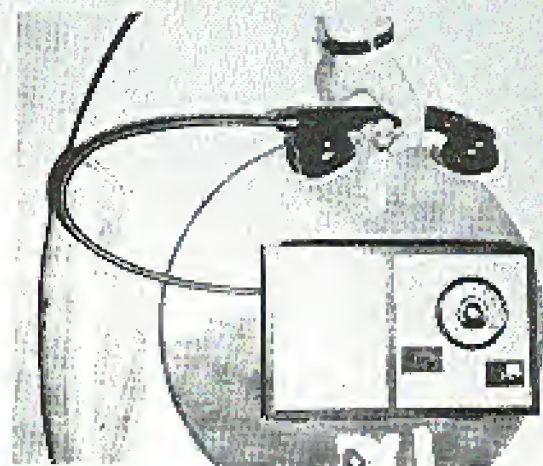
SECOND CLASS POSTAGE
 Permit Paid at
 East Setauket, N.Y.
 11733
 ISSN 0748-3151

2600

The Hacker Quarterly

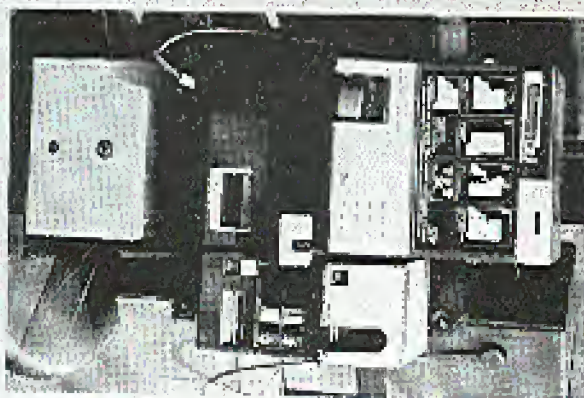
VOLUME EIGHT, NUMBER THREE
 AUTUMN, 1991





A Polish Gayphone in Warsaw

Photo by Tom Blauke



Orange payphones in Italy. An increasing number only take cards.

Photo by John Durkin

SEND YOUR PAYPHONE PHOTOS TO: 2660 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NT 11951. STILL WAITING FOR AFRICAN PAYPHONES

[illegible]

2600 (ISSN 0744-1455) is published quarterly by 2600 Enterprises Inc., 7 Strong Lane, Scarsdale, NY 11733. Second class postage permit paid at Scarsdale, New York. POSTMASTER: Send address changes to:

Copyright (c) 1991-2000 Entomprises, Inc.

Yearly subscription: U.S. and Canada --\$21 individual, \$50 corporate (U.S. funds)

Overseas -- \$310 million, 25% corporate

Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990 at \$25 per year, \$30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:

2660 Sunnington Dr., P.O. Box 752, Middle Island, NY 11935-0752

FOR LETTERS AND ARTICLES SUBMISSION, WRITE TO:
2610 Editorial Dept. P.O. Box 99, Melville, NY 11767-0099

20000 Chantrelle Dr., Dept. 1, Box 1000, 75210-1000
NETWORK ADDRESS: 35100well@csuhs

NETWORK ADDRESS: 2500@well.sf.ca.us

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-751-2602

Why Won't They Listen?

By this time, we've all And why is there so much gross witnessed some kind of media negligence?

Whether it's the piece in your newspaper about kids with computers figuring out how to make free phone calls or the special report on television that shows how hackers can gain access to secret corporate computer networks, the angle is almost always the same. And it usually misses the most important point: What kind of data is being stored? Why is it so easy to gain access?

Our first story concerned access to U.S. military computer

systems. Over the past few years, Dutch hackers have been able to get into all kinds of systems. This is not because they're necessarily better than American hackers. But they do live in a healthier society where curiosity and exploration are encouraged, not punished. We asked them to show us on videotape just how easy it was to get into a military system. They graciously did this and even we were surprised at how easy it was.

By going to the media and showing them this, we thought that hackers might finally be seen in a better light. After all, with knowledge of military weaknesses, there are plenty of places these hackers could go. But they didn't. They chose to share the information.

Our other story concerned pushbutton locks that are appearing everywhere we look. And while technically this had nothing to do with computers, the similarities were astounding. Here we have a gadget that is supposed to provide security. The average person looks at it and believes what they're told, in much the same way they would believe what a computer tells them without question. But hackers discovered that there was something seriously wrong here. The upshot of our story was that these locks were not locks at all, but open invitations to disaster.

Again, going to the media with this story seemed the proper course of action. Instead of using this knowledge for our own gains, we realized that people had to be warned before it was too late.

These locks, which have been used in businesses and offices for years, are now being installed in homes. We knew the media would understand the threat.

What can we say? We were wrong. Despite a massive effort on our part to get every media outlet in the country involved in these stories, the interest we received back was negligible. We held a press conference in New York City, made hundreds of phone calls, did tons of research, and are still paying the bills for it. And it's likely you never heard a single word about it. They decided it just wasn't something the American people needed to hear.

Ironically, in subsequent weeks there were stories in the media of Dutch hackers invading computers yet again. The same old angles. No mention of the efforts of hackers to safeguard these systems. That just wasn't newsworthy.

We think things will change when computer systems with sensitive information are accessed by malevolent people who know what they're doing. They'll change when homes, offices, schools, and mailboxes around the nation are broken into without a trace. We believe that then and only then, the media will take an interest. And, of course, they'll probably decide to blame us. The ratings and circulation will go through the roof.

We did our best to warn the American public of two distinct dangers. It's now up to our readers to spread the word where the media won't.

STAFF

Editor-in-Chief

Emmanuel Goldstein

Artwork

Holly Kaufman Spruch

*"They are satisfying their own appetites to know something that is not theirs to know."
Asst. District Attorney Don Ingraham*

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Eslov, Mr. French, The Glitch, Bob Hardy, The Infidel, Kevin Mitnick, Knight Lightning, The Plague, David Rußerman, Bernie S. Scott Skinner, Silent Switchman, Mr. Upsetter, Dr. Williams, and those who are elsewhere.

Remote Observations: Geo. C. Tilyou

Shout Outs: Jim Ross, Simplex (for the hours of fun), Len Rosa, Franklin, Strong Island Resistance.

SIMPLEX LOCKS

AN ILLUSION OF SECURITY

by Scott Skinner and
Emmanuel Goldstein

No lock is one hundred percent secure. As any locksmith will tell you, even the best lock can be opened if one wishes to invest the time and resources. However, a good lock should at least be secure enough to prevent the average person from compromising it. Common sense dictates that a lock which can easily be opened by anyone is simply not a safe lock to use.

While an average person may not have the necessary skills and expertise to use a lock pick or a blowtorch, almost everyone has the ability to count. And the ability to count is all that is necessary to compromise a Unicam/Simplex pushbutton lock. In addition, one needn't count very high. Only 1085 combinations are used, and in most cases this number is reduced considerably.

Anyone can easily open a Simplex lock by merely going through all the possible combinations. As tedious as this may sound, members of 2600 average ten minutes when put to the task. This method becomes even easier if one can find out the "range" of the combination. For instance, if one knows that only three pushbuttons are being used, then one merely has to go through 135 combinations. In this example, a Simplex lock can be compromised in under five minutes. With some models (particularly the commonly used 900 series), a new combination can then be set without a key. One can literally lock someone out of their own home.

Far worse than the low number of combinations is the illusion of security that surrounds the lock. We called ten locksmiths at random and were told that "thousands," "millions," and in some

cases "a virtually unlimited number" of combinations were available. These claims are somewhat misleading considering the actual number of possible combinations. In addition, no locksmith was able to tell us exactly how many combinations were available, nor did any locksmith believe us when we told them.

Simplex advertisements also claim that these "maximum security" locks are "ideal for security-sensitive areas" and that some models meet the requirements of the Department of Defense Security Manual. We contacted Simplex to find out just what these requirements are. According to Thomas Nazzio, Vice President of Marketing, the locks comply with paragraph 356 of the Department of Defense Security Manual (DoD 5230-72-M). Mr. Nazzio's refusal to quote paragraph 366 of the manual as he felt it was "restricted." However, he summarized the section by claiming that Simplex locks comply with the DoD Security Manual for security-sensitive areas.

2600 was able to obtain a copy of this "restricted" manual just by asking. Upon close examination of paragraph 366 entitled "Automated Access Control Systems," we were unable to find any information concerning mechanical pushbutton locks. The section that does apply to Simplex locks is paragraph 366 entitled "Electric, Mechanical, or Electromechanical Devices." According to this section, mechanical devices which meet specified criteria may be used "to control admittance to controlled areas during working hours." (emphasis added) While there is an element of truth in Mr. Nazzio's claim, he did not tell us that according to the DoD Security Manual, Simplex locks may not be used as the only

lock source except during "working hours." In addition, it is relatively easy to meet the requirements of the DoD Security Manual. Virtually any combination lock with changeable combinations, and indeed even padlocks, will meet these requirements.

Although Simplex claims that "thousands of combinations are available," in truth only 1085 combinations are used. Another 1085 combinations are available in the guise of "high security half-step codes." These are codes which require the user to push one or more buttons only halfway. Because of the extreme difficulty in setting and using these half-step codes, Simplex advises against their use, and in most cases, does not even inform the user that these codes are available. According to one locksmith, "[Simplex] only suggests it for really high security installations. Government installations. For the average consumer, they don't want anyone to know about it."

We shudder to imagine which high security government installations are using Simplex locks as the only lock source. The "high security codes" are an example of misleading information being used to sell the locks (in this case, to the U.S. government). Naturally, the addition of 1085 combinations does not make the lock considerably more secure. (If 21710 combinations seems like a large number, consider that a S5 Master lock has 64,000.) In addition, we have yet to find one single instance where the half-step codes are used.

We have found that numerous organizations use Simplex locks as the primary lock source. Among the guilty parties in the New York metropolitan area are Federal Express, United Parcel Service (UPS), Citicorp Center, John F. Kennedy International Airport, and the State University of New York at Stony Brook. Others around the nation include General

Motors, the State Department, McDonalds, NSA, and the University of Wisconsin.

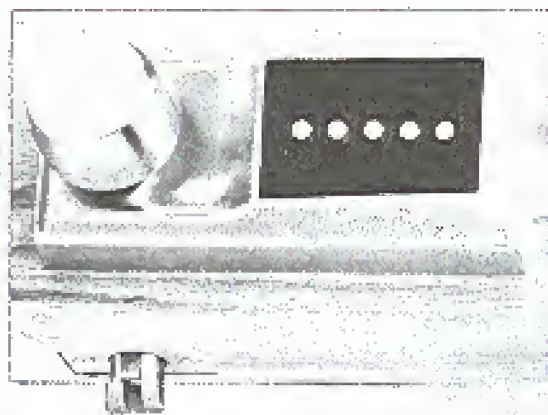
The biggest offender is Federal Express, which uses Simplex locks on over 25,000 dropboxes nationally. According to Robert G. Hamilton, Manager of Corporate Identity [sic] for Federal Express, "[Federal Express dropboxes] are extremely secure. As a matter of fact, there's probably double the cost of security built into those boxes than what's necessary. The idea of having somebody put something extremely important and vital — and it's obviously important and vital or they wouldn't ship it Federal Express — in one of these security was upmarket on people's minds.... [The dropboxes] are like vaults." These "vaults" were accessed by members of 2600 in less than ten minutes.

The dropboxes are particularly insecure because Federal Express uses the same combination for all of their dropboxes in every state on the east coast! So by opening one dropbox, we now have access to thousands.

Members of 2600 also gained access to a UPS dropbox — in one shot. UPS did not even bother to change the default combination which is set by Simplex. And just like Federal Express, UPS figures that a single combination is good enough for every dropbox.

Another big offender is the State University of New York at Stony Brook, which uses Simplex locks in both dormitory and academic buildings. According to University Locksmith Gerry Lema, "I don't consider [the Simplex lock] to be a secure lock. I prefer a deadbolt lock which operates with a key more than I would a Simplex lock.... I think it's more of a convenience lock than it is a security lock." When asked why the university continues to use the lock, Mr.

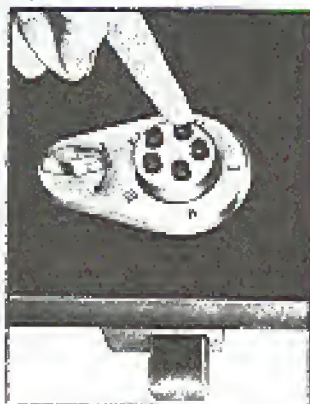
Simplex Series 1000



"The dropboxes are the vaults." - Federal Express



Simplex Series 900



SIMPLEX LOCKS
TOUCH US ALL,
EVERY DAY.
PLEASE TELL US
WHERE YOU FIND
THEM IN YOUR
AREA.

Simplex® AUXILIARY LOCKS

OPERATING INSTRUCTIONS

All locks are shipped with the following combinations:
11 and 12 (control) and 100000 (main).

1



Turn the front control knob clockwise "SIMPLEX" to the LEFT, and release.

2



Press the control buttons in the proper order.
Release buttons before turning control knob.

3



Turn the control knob RIGHT to open.
To lock — turn the control knob LEFT. (Model 54, lock automatically.)

CHANGING COMBINATIONS

You may change combinations to any sequence you wish — using any of six buttons in any order, separately or pushed at the same time with other buttons. You cannot use the same button more than once in a combination.

1



With the door open and the "SIMPLEX" lock locked, turn door control knob clockwise "SIMPLEX" to the LEFT, and release. PULSE THE EXISTING COMBINATION AND RELEASE BUTTONS.

2



Remove the screw in the lock housing with the Allen wrench provided. Insert the screw into the hole and depress the button finger wrench.

3



Turn the front control knob clockwise "SIMPLEX" to the LEFT, and release.

4



Press the buttons in the sequence desired for your new combination — single and alternately. Record your new combination.

5



Turn the front control knob RIGHT. Your new combination is now installed. Before closing the door, try it to be sure you have installed it correctly. Re-place the threaded screw in the lock's housing.

NOTE: If the front control knob opens the lock without passing the combination, steps 2, 4 and 5 were performed out of order and your "SIMPLEX" is not a "B" combination. To install a combination, follow the above instructions step 1.

The front control knob can NOT be forced to open the lock, except if it is connected to the lock. If the lock is broken through, if the screw has been forced, it will be damaged and can be moved back to the screw position by hand or with a pair of pliers without damaging the lock.

Pat. No. 3940554 - Page 2 of 6A

Simplex Security Systems, Inc.

10000 10000 10000 10000 10000 10000 10000 10000 10000 10000
10000 10000 10000 10000 10000 10000 10000 10000 10000 10000
10000 10000 10000 10000 10000 10000 10000 10000 10000 10000

Lenox said, "The university did not consider contacting the university locksmith on his expertise. I had originally told them years ago when the Simplex locks were first introduced not to use [the locks] in the dormitories." Not only are they being used in the dormitories, but the university is considering purchasing 1500 more for additional rooms.

The illusion of security Simplex is portraying with misleading advertising is that Simplex locks are just as secure, if not more secure, than key locks. The result of this myth is that many businesses, institutions, and homeowners confidently use Simplex locks as the only lock source despite the fact that the locks are inherently insecure. Even when locksmiths are consulted, we have found that they simply perpetuate the illusion of security by claiming that Simplex locks are "top of the line" and that "even the Department of Defense uses them." Nowhere is it mentioned that Simplex locks should never be used as the only lock source. Even worse, Simplex is now aggressively pursuing the homeowner market with their new "residential" 6000 series. These new locks employ the same insecure mechanism, and are being marketed as primary locks.

Realistically, Simplex locks are more of a convenience lock than anything else. They are convenient because they do not require keys and the combinations are easily changed. However, this convenience backfires when it comes to security. These locks are so convenient that people tend not to use other locks that may also be present on the door.

For those organizations currently using Simplex locks, we recommend following the guidelines of the DOD Security Manual: the locks may be used as the sole lock source only during working hours. For home or private use, we strongly advise that consumers use these locks in

conjunction with a key lock and never as the sole means of security.

Hacking Simplex Locks

In this issue is a list of all possible combinations for Simplex locks. We have divided the list into four groups according to how many pushbuttons are used. The numbers listed in parentheses refer to pushbuttons that must be pressed together. If you find that none of the combinations appear to open the lock, then it may be a rare instance of a half-step code. In this case, only the last number (or numbers if they are in parentheses) should be pressed in halfway and held while the knob or latch is turned. Slowly press in the pushbutton(s) until you feel pressure. If you hear a click then you have pushed the buttons in too far. If all of this sounds complicated, then you are beginning to understand why it is that Simplex does not recommend the use of half-step codes, and subsequently why half-step codes are virtually never used.

Simplex locks come in many different shapes, sizes, and colors. However, the two models that you will most likely see are the 900 and the 1000 series. The characteristic features of the 900 series are five black buttons spaced in a circular fashion on a round, movable cylinder. In addition, the 900 series utilizes a latch instead of a doorknob. The 1000 series is much larger, with five (usually metallic) pushbuttons spaced vertically on a rectangular metal chassis. Unlike the 900 series, the 1000 has a doorknob.

We suggest that novice attempt their first hack on a Simplex 900 model. If the latch is located below the buttons, then the procedure is as follows: (1) turn the latch counter-clockwise to reset the lock; (2) enter a combination from the list; (3) turn the latch clockwise to open. If the latch is located above the buttons then simply reverse the procedure. Make sure that you reset the lock after each try.

To hack a 1000 model, simply enter a combination from the list and turn the knob clockwise. You will hear clicks as you turn the knob, indicating that the lock has been reset. It is sometimes difficult to tell when you have cracked a 1000 model by simply turning the knob. When you do get the correct code, you will hear a distinctive click and feel less pressure as you turn the knob.

You will find that turning the latch on a 900 model requires less wrist motion and makes much less noise than turning the knob on a 1000 model. These details seem trivial until you realize that you may have to turn the latch or doorknob a few hundred times before you crack the lock.

We cannot stress enough how much easier it is when you know the range. For instance, if you know that only three digits are being used, then you do not have to waste time trying four digits. One way to find out the range is to stand nearby while someone punches in the code. You will hear distinctive clicks which will give you an idea of the range. If you cannot stand nearby, then try listening a voice activated tape recorder near the door. The tape recorder will remain off until someone comes up to punch in the code. You can then retrieve the recorder later at your convenience and listen for the telltale clicks. We find that this method only works in quiet areas, such as the inside of a building. Another way to find out the range is to take a pencil eraser and carefully rub off a tiny bit of rubber on each of the pushbuttons. When someone comes to enter the combination, they will rub off the rubber on all of the pushbuttons that they use, while leaving telltale traces of rubber on the pushbuttons that they do not use. This method works particularly well because you eliminate pushbuttons, which drastically reduces the number of combinations that must be tried.

We find that certain ranges tend to be

used more than others. Group B (three pushbuttons) tends to be used in "low security areas," while Groups C and D tend to be used in areas which seem like they should be more secure. We have never found a lock which uses a combination from Group A. For some reason, we find that the 1000 series mostly uses Group C (four pushbuttons). In addition, most combinations tend to be "doubles," which require at least two of the pushbuttons to be pressed together. When you focus on a particular range in strict with, try the doubles first. For instance, try "(12) 3 4 5" before you try "1 2 3 4 5." We have never found a lock which uses a triple, quadruple, or all five pushbuttons pressed at the same time.

Although we are providing a list of all the possible combinations, you may find it useful to invest some time and record these codes onto cassette. This makes it much easier for one person to hack a Simplex lock because he does not have to hold the codes in one hand while hacking, nor cross out the codes to keep his place. A notebook also looks far less conspicuous than boxes of paper filled with numbers. The only drawback to using a walkman is that the person hacking will not be able to hear anyone coming from a distance. We find it easier to hack Simplex locks in small groups, so that each person can take turns, and everyone has their ears open.

Finally, it is always good to take a few lucky shots before you initiate a brute force hack. Always try the default combination "(24) 3" before you try anything else. Above all, don't give up! Even if you do not get the combination in ten minutes, you are still that much closer to figuring it out. We recommend that you do not stress yourself out trying every combination in one shot. A few minutes a day will do just fine, and the thrill of achievement will be well worth the wait.

The Hacker Video

Over the summer, military computer systems in the United States were accessed by Dutch hackers. One of the episodes was captured on videotape by 2690, partisans of which were shown on a recent nationwide television show. Most of it, however, has never been seen. We are releasing this videotape to the public so that more people will witness just how shamefully easy it is to get access to military computers.

The intrusion took place in late July of this year. The purpose of this demonstration was to show just how easy it really was. Great care was taken to ensure that no damage or alteration of data occurred on this particular system. No military secrets were taken and no files were saved to a disk by the hackers. What is frightening is that nobody knows who else has access to this information or what their motivations might be. This is a warning that cannot be taken lightly.

Explanation of the Videotape

The tape opens with some background shots of the hacker site in Amsterdam. Basically, it's a group of about five people in their twenties gathered together to watch vids and play with computers.

Through a local phone number, a connection is made to the Internet. This network ties together schools, corporations, and government installations around the world. By connecting from one machine on the Internet to another, you can use two or more computers at once, without a

noticeable loss of speed.

telnet 192.67.67.20

Using a program called "telnet", the hackers connect to the Defense Data Network Information Center. (Telnet enables a user to actually login to systems all over the world.) In this case, the particular address is "192.67.67.20", a computer which requires no password and is open to everyone. (The address has since been changed to 192.112.36.5.) It is a clearinghouse of information about various systems and their users.

The hackers are met with a "Whois?" prompt. The computer is asking them who they want to have checked out. The hackers type "army.mil", indicating any computer on the military network that has the word "army" in its address. The computer spits out over one thousand computer names and addresses.

A computer named "tracer.army.mil" at address 192.33.5.135 is chosen at random. (This computer is believed to be located at Los Alamos, but this has not been confirmed.) The hackers then begin to try default passwords, like "guest", "public", "uucp", etc. None of these work.

ftp -n tracer.army.mil

The next line of attack is the ftp command. By using ftp (file transfer protocol), anyone can copy files from one system to another. Ftp is similar to telnet in that it connects to systems all over the world. But

while telnet is used to login to systems, ftp is only used to transfer files. In addition, it is not necessary to have accounts on more than one machine in order to use ftp.

The way it works is as follows: a user logs into a machine on the Internet. Using ftp, he connects to another machine, which then asks him for a user name. By typing "anonymous", the user is granted limited access to the machine. The purpose of this is so that public files can be made available without having to give out accounts to everyone needing access.

quote user ftp
quote cwd -root
quote pass ftp

But this version of ftp has at least one major bug in its software. By issuing the above commands, the user is not only able to gain access to the machine, but change his directory (location) on the system to the root directory. (Root is the most powerful account on the system.) So instead of being able to look at a limited number of files on the system, the anonymous user is now able to look at anything. In addition, the hackers can also change anything, albeit with great difficulty. This is because the hackers are not actually logged into the system. They are still confined to working within the framework of the ftp program.

At this stage, while the hackers can read and alter any bit of information on this military system, they cannot run any programs. Also, they cannot actually login to the system. But this doesn't remain a problem for very long.

get /etc/passwd
exit ftp and modify password file on home system

Since ftp allows users to copy files, the hackers choose to copy the password file (known as "/etc/passwd"). This file contains a list of every user on the system along with their encrypted password. It is virtually impossible to actually decrypt these passwords, which is why the file is readable by any user on the system. (It is not supposed to be readable through ftp, however.) Ordinarily, copying this file would not be very significant. However, once the hackers have the file copied to their home system, they carefully insert another user into it. Since the system believes they have certain privileges, it allows them to replace the old version of the password file with their new version.

The user name they create is "dquayle". In the field where the encrypted password would be is nothing. This means there is no password for Dan Quayle's newly created account. Hence they do not have to worry about decrypting it. The hackers apparently had intended to give dquayle root privileges by inputting the appropriate values for his account. But a careful look at the videotape will show that dquayle was not given any special privileges.

ftp -n tracer.army.mil
quote user ftp
quote cwd -root
quote pass ftp
put /etc/passwd
exit ftp

The hackers repeat the first series

of steps (henceforth known as the "flip bug") to once again get root privileges. The original password file is now replaced with the modified version containing the fictitious user "dquayle".

telnet tracer.army.mil

The hackers reconnect to the military system, which asks for a username. The hackers type in "dquayle". Access is granted without a password.

But root access is not granted. Instead, a warning is printed on the screen indicating that the terminal is "not a secure device". In many cases, the system will not allow root access to anyone coming in from the outside. This was what originally appeared to have happened. However, as mentioned earlier, duquayle had no special privileges; as the system never even tried to access the root. Either way, it would seem that the hackers' ultimate goal has been thwarted.

exit telnet and modify password file on target system.

flip -n tracer.army.mil

quote user flip

quote cxd -root

quote pass flip

put /etc/passwd

exit flip

Instead of giving up, the hackers go back to their copy of the password file. They make another account, this time with root privileges and no password. This account they call "tebor", the word root backwards. They once again make use of the flip bug to "put" the new password file on

the system.

telnet tracer.army.mil su tebor

Using telnet, the hackers once again login as duquayle. This time, after the warning is issued, they issue a two letter command ("su") followed by their new user ("tebor"). The su command allows a user to switch to the identity of another user while logged in. It solves the trouble of hanging up and calling back into the system and is useful if someone has two accounts or if two users are sharing a terminal. In this particular case, the hope is that the su command will not check to see if the call was coming from outside.

No password is requested since none was entered into the root account. A single "*" on the screen tells the hackers that their mission has succeeded. That symbol indicates true root access. The su command granted them root access even though they were coming in from the outside. Since they were already logged onto the system, su assumed they were legitimate. This military computer system (tracer.army.mil) is now completely under the hackers' control.

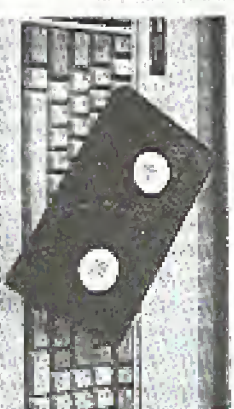
The rest of the night is spent looking for interesting bits of data to prove beyond a doubt that this is not a system for just anyone to be in. The next day, some of the data is scrolled through. Among the more interesting pieces is a memo from the Counterterrorism Officer dated January 16, 1991 (the deadline day for Iraqi troops to be withdrawn from Kuwait) discussing security issues. Clearly, this is sensitive information.

How Passwords Are Guessed

The final part of the tape illustrates a password hacker program. Using the aforementioned password file, the program comes up with the most commonly used passwords. Instead of decrypting the passwords in the password file, it encrypts the possible passwords (the encryption algorithm is standard) and then compares them to the actual passwords. If they match, then a password has been found. In the example shown (from a different system), many passwords are found in this manner.

Why We Are Exposing This

The hackers responsible for this are not interested in military secrets. But they do recognize the importance and value of the information that is stored on such



A portion of the videotape

computers. The fact of the matter is that if these gaping security holes are not openly exposed, they will never get fixed. Ironically, the bug that was used in this particular case is a fairly old one that has been fixed on most systems. Why it still existed on a military system is beyond us. But we do know that this is only one system and only one bug.

Corporate computer systems also

continue to operate with security holes. As hackers, we are concerned with the lack of safeguards that are being placed upon sensitive data. In addition to military data, much information about individual people continues to be shoddily managed. Our credit ratings, telephone records, banking information, and computerized files of all sorts are open to scrutiny for anyone who can gain access.

We should stress that the vast majority of unauthorized access does not involve computer hackers. Since we have no ulterior motives, other than the quest for knowledge, we openly reveal whatever we find out. Unfortunately, this often results in our being blamed for the problem itself — confusing the messenger with the message. In reality, there are countless instances of employees invading the privacy of individuals by accessing credit files or billing information that they have no business seeing. Since this information is so easy for them to get ahold of, there is virtually no way of their being detected. And, even if they were detected, they aren't really breaking any laws.

Add to this the increasing fragility of our modern technology as computers become dependent upon other computers and it becomes evident that serious problems, even catastrophes, lie ahead. The actions of computer hackers are, at worst, an annoyance to some rather powerful people. Were we not to expose the flaws in the system, they would still be there and they would most definitely be abused.

We will send you a VHS copy for \$10 or 3 black and white tapes.

protecting your ssn

by Chris Hibbert
Computer Professionals for
Social Responsibility

Many people are concerned about the number of organizations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being tracked as just a number.

Unfortunately, I can't offer any hope about the dehumanizing effects of identifying you with your numbers. I can try to help you keep your Social Security Number from being used as a tool in the invasion of your privacy.

Surprisingly, government agencies are reasonably easy to deal with; private organizations are much more troublesome. Federal law restricts the agencies at all levels of government that can demand your number and a fairly complete disclosure is required even if its use is voluntary. There are no comparable laws restricting the uses non-government organizations can make of it, or compelling them to tell you anything about their plans. With private institutions, your main recourse is refusing to do business with anyone whose terms you don't like.

Short History

Social Security Numbers were introduced by the Social Security Act of 1935. They were originally intended to be used only by the Social Security program, and public assurances were given at the time that use would be strictly limited. In 1948 Roosevelt signed Executive Order 9397 which required federal

agencies to use the number when creating new record-keeping systems. In 1963 the IRS began to use it as a taxpayer ID number. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their databases and required disclosures (detailed below) when government agencies request the number. Agencies which were already using SSNs as an identifier were allowed to continue using it. The Tax Reform Act of 1976 gave authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. The Privacy Protection Study Commission of 1977 recommended that the Executive Order be repealed after some agencies referred to it as their authorization to use SSNs. I don't know whether it was repealed, but that practice has stopped.

The Privacy Act of 1974 (5 USC 552a) requires that any federal, state, or local government agency that requests your Social Security Number has to tell you three things:

- 1: Whether disclosure of your Social Security Number is required or optional.
- 2: What law authorizes them to ask for your Social Security Number.
- 3: How your Social Security Number will be used if you give it to them.

In addition, the Act says that only federal law can make use of the Social Security Number mandatory. So anytime you're dealing with a government institution and you're

asked for your Social Security Number, just look for the Privacy Act Statement. If there isn't one, complain and don't give your number. If the statement is present, read it. If it says giving your Social Security Number is voluntary, you'll have to decide for yourself whether to fill in the number.

Private Organizations

The guidelines for dealing with non-governmental institutions are much more tenuous. Most of the time private organizations that request your Social Security Number can get by quite well without your number, and if you can find the right person to negotiate with, they'll willingly admit it. The problem is finding that right person. The person behind the counter is often told no more than "get the customers to fill out the form completely."

Most of the time, you can convince them to use some other number. Usually the simplest way to refuse to give your Social Security Number is simply to leave the appropriate space blank. One of the times when this isn't a strong enough statement of your desire to protect your number is when dealing with institutions which have direct contact with your employer. Most employers have no policy against revealing your Social Security Number; they usually believe the omission was an unintentional slip.

Lenders and Borrowers

Banks and credit card issuers are required by the IRS to report the SSNs of account holders to whom they pay interest or when they charge interest and report it to the IRS. If you don't tell them your number you will probably either be refused an account or be charged a

penalty such as withholding of taxes on your interest.

Insurers, Hospitals, Doctors

No laws require medical service providers to use your Social Security Number as an ID number (except for Medicare, Medicaid, etc.). They often use it because it's convenient or because your employer uses it to certify employees to its group health plan. In the latter case, you have to get your employer to change their policies. Often, the people who work in personnel assume that the employer or insurance company requires use of the SSN when that's not really the case. When my current employer asked for my SSN for an insurance form, I asked them to try to find out if they had to use it. After a week they reported that the insurance company had gone along with my request and told me what number to use. Blood banks also ask for the number but are willing to do without it if pressed on the issue. After I asked politely and persistently, the blood bank I go to agreed that they didn't have any use for the number, and is in the process of teaching their receptionists not to request the number.

Why Use of Social Security Numbers is a Problem

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't as all secure; if someone makes up a nice-sight number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants); or

to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally printing a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers. (One is given below.)

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whatever record it shows up on. When it happens accidentally, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

What You Can Do to Prevent

Your Number

If despite your having written "refused" in the box for Social Security Number, it still shows up on the form someone sends back to you (or worse, on the ID card they issue), your recourse is to write letters or make phone calls. Start politely, explaining your position and

expecting them to understand and cooperate. If that doesn't work, there are several more things to try:

If talk to people higher up in the organization. This often works simply because the organization has a standard way of dealing with requests not to use the SSN, and the first person you deal with just hasn't been around long enough to know what it is.

2) Enlist the aid of your employer. You have to decide whether talking to someone in personnel, and possibly trying to change corporate policy, is going to get back to your supervisor and affect your job.

3) Threaten to complain to a consumer affairs bureau. Most newspapers can get a quick response. Some cities, counties, and states also have programs that might be able to help.

4) Tell them you'll take your business elsewhere (and follow through if they don't cooperate).

5) If it's a case where you've gotten service already, but someone insists that you have to provide your number in order to have a continuing relationship, you can choose to ignore the request in hopes that they'll forget or find another solution before you get tired of the interruption.

If someone absolutely insists on getting your Social Security Number, you may want to give a fake number. There is no legal penalty as long as you're not doing it to get something from a government agency or to commit fraud. There are a few good choices for "anonymous" numbers. Making one up at random is a bad idea, as it may coincide with someone's real number and cause them some amount of grief. It's

better to use a number like 078-05-1120, which was printed on "sample" cards inserted in thousands of new wallets sold in the 40's and 50's. It's been used so widely that both the IRS and SSA recognize it immediately as bogus, while most clerks haven't heard of it. It's also safe to invent a number that has only zeros in one of the fields. The Social Security Administration never issues numbers with this pattern. They also recommend that people showing Social Security cards in advertisements use numbers in the range 587-55-4320 through 987-65-4329.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.

[illegible]

Where One Hacker Went

The "White House All The Freedom Cries" article in the Summer 1991 issue was relevant and generally powerful enough to bring me temporarily out of the "woodwork." I admit my guilty of the article's disregard of "backers" legitimizing its message in terms and remaining underground like criminals.

Curious to some of the things I've had to do in the past, I was ever present, never had my house searched, nor had anything confiscated. The less security is an absolute miracle due to the many things I've had to do, and I'm not a person who is security and law enforcement people who are not going to get the "Guns" or "Laser" and not have ever betrayed the trust of those who were then colleagues to avoid trouble with the law.

Perhaps my belief in freemason lodge and its accompanying activities, and also my alleged sexual desire, preoccupied with a computer and modern, was what preoccupied me with the past. There were a number of similar issues, distributed chronologically, which I attempted to inform those who wanted to join about the use and abuse of various technologies, and what I saw as my affiliation with the Legion of Christ helped to change the discourse.

I can't say that my ego had nothing to do with writing "Eldes," as being recognized among Americans, however distant, as they may have been, was important to me. The drive to "be there" had some pull too. On the other side of the coin, had some push too. I don't want to call it a system by informing people of the inequity of corporate America was more of a factor in writing it than my ego was however. In retrospect, I realize that I was the worst who needed the thing and not the best.

For me, as a 70-year-old, I did not use a modern language program; this, according to the same *Star* that was mentioned in the article, "The Frank Bookend," is a "pastime of my own hobby" with the obvious difference being that I am a free person. I will always live with the reality that my past misadventures may one day catch up with me. I never printed "secretary" and I never acted with malice when I used my computer and modem. Yet I am still fearful it supports a man's notion of my own cowardice, the kind of a challenge, and the prohibition of trying to influence others of what was not true. I was no "persecuted" nor "each criminal."

Today I use computers sparingly. Like most people, my computer use is limited to sending e-mail with tasks that we can't refuse to do "manually." And for the record, against I teach a computer it is best to stick to the basics only. It appears to me that as time goes on, older people become more efficient. In my opinion, those who did it the "old" way are a threat.

always a chief" are erroneously imagined, narrow-minded, and discussing of literature as a whole, including themselves. People can add to the go,

[illegible]

It would be interesting to see a bulletin board that discussed banking topics with some of the "odd interest" who have gone underground along with the newly curious while circulating within the boundaries of the law. But what the current state of needed civil ignorance and "don't ask, don't answer" mentality, only the chance of people would agree to run it.

[illegible]

I am still a hacker in the pure sense: being curious, trying new approaches to problems, expanding the envelope, etc. The hacker in the dark sense is dead. Forgive me that, partly due to immaturity, partly due to self-grooming, partly due to the realization that the ends do not justify the means.

[illegible]

Technical Questions

Why would I pay \$6.30 an hour via subscription rather than the \$6.00 one-and-done price?

I'm not complaining. You pay prices don't make sense. Good is the lifetime subscription price \$580 so far exceeds per year means that it won't begin to pay for 55 years. Also, why should a corporation pay more for a subscription than to individually?

I am glad to see your magazine on my television screen. Hope you become as big as *Playboy* and other body magazines.

MOC
Mestlin, TX

The name *phyllo* is known as a shortened alternative.

that if you do not do any individual work, the do not do some exercises with you the way that, higher pressure need to do something else kind of thing. The advantages to doing group are convenience and flexibility. Furthermore, generally get their opinion at least a word before any individual do. As to why corporations say more than individuals, we find that large organizations require a substantial amount more information than individuals. Furthermore, decision making need, and show skills are a normal part of the corporate world. He thought more to cover all of this and also human many organizations spend more resources to many different individuals. A special case for individual representation relate within an organization.

environment is certainly not a bad deal. Regarding the life-time subscription, it actually would begin to pay in just over 15 years, not 65. But that's not the point. *Life-time subscriptions are far above what we want to pay and so make a significant contribution to our cost-based operations. If we're not for these people who sleep in the past, it would be a significantly worse deal than we are now. We are disturbed to hear that result for their generation.*

Raw Data

This is *Wunder* (he's a service for *Shimmer*). I got it by directing to the assistant on Mr. Elanor's & *Shimmer*. I suggest if you get it, they'll change it, but don't fret.

The Millionaire Midnet
By printing it, we take for people leave it clear in
the first place, if it isn't shared, there's no reason for
it to be changed.
(Mar 2000)

if the Milne-Milne

For example, "Out the receiver off the phone if possible or, if not possible, turn the phone off," he said. "If you can't do that, get out the phone line coming into the COCOT. I usually cut the COCOT cover and he sold his phone. We're extremely sensitive to lighting and electrical items. The more things there were, the better it was."

He had to check his COO's office to see if the mile-thin ops team could handle the speaker of the phone with a sharp note and then connect a device such as an electronic opus lighter that doesn't glow by starting barbecue fires, one could probably screw up the mile thin. Save your course and still have food!

Arkansas Loan Collector

Thank you again about COX-2, as we continue to use the PGE and still do because it hasn't been implemented here yet. If you believe that's the problem, the COX-2 is the solution to this problem, not if I try to know what you have planned for the next ATAT meeting. Perhaps finding the state of New Jersey. Multiple other kinds of "nonlinear" may make you feel better. They really don't do much to solve the problem. The COX-2 concept used to be well understood, just like the physical components. But many of us need to also know the physical components. COX-2's values are found with some of the problems. COX-2's values are found with

Because of unfair practices by the phone companies, COCO-OTV don't have access to the same technology that "regular" people have. Therefore, all of the technology must be built into the phone itself. If the system was really fair, the billing and routing information would not be controlled by a company that also operated the phone. Obviously that phone will get preferential treatment and the others will suffer. It's in the interest of the phone companies to make COCO-OTV an independently owned phone. Think about this the next time you blow one up.

Dear 2600:

As most of us know, the 800-443-3148 ANI seems like a dead end. I've been trying to get a hold of the person in charge of the ANI system, but only with a price request (which I will get the same office (817-671-5629) to inform them that your "General ANI customer" would like a live demo of their ANI system software, and their office will contact MEI, who will in turn allow ANI access for a designated period (usually three hours at a time). Probably not without MEI. Seriously, I'm going to the challenge. Thus, there may be some experimentation to this method.

A little of info on Avcon Logic Technologies: the president (Joe Sargent) is also Vice-Chairman of the Board for the Tandy Corporation. Now that is a very interesting item.

There is yet another procedure for ANI. Emergency 24, a nationwide alarm monitoring service in Chicago has two 800 access lines: 800-382-0911 weekdays and 800-447-5161 weekends. Upon activation, a live operator will request the number you are calling from, through 800 ANI. To allow some recognition, you may be asked to "enter department voice mail," and your call will be forwarded at that point. The save the call is logged somewhere with AT&T. The ANI would request of whether the call is direct dial or operator assisted. Take two 800 numbers are AT&T provided, and the ANI information is processed despite the routing procedure. Placing the call through alternative carriers delivers the same end result.

Bellcore has a new publication listing of Tech Support. "The Catalog of Technical Information" is a book for one's bookshelf. A call to 800-331-2613 has been established for a copy of their listing and for more. Telsone Corporation of Boothell, WA has a "Telsone Design Solutions Catalog" for free with a call to 800-426-8976. Some interesting "application notes" can be found at the end of this major data supply catalog.

Finally, a couple of queries. Any modern know of any methods not known to block the ANI information on 800 calls? The service is available to all 800 subscribers, either with internal call-routing and reporting, or with a separate reporting system. First time users where ANI services are not yet available, it seems feasible that you could become an 800-443-3148 subscriber, have the CO number-forward the call to your own number, and with ANI 800 ID

hardware and software, well, ANI. Do any modern know if it will actually work in application mode?

OS
Seattle

FAXers Beware

Dear 2600:

I just recently received my first issue of 2600 and I enjoyed it very much. However, I was dismayed to see the box on page 45 about having a message. For transmissions are no other than regular voice, as far as that matter, data transmissions. There is an entire industry of facsimile encoding and decoding devices. One device, known as the STG Remote Satellite Logging System, is most for law enforcement only, but the company will sell a for-profit. According to its description, "The Satellite Logging System is designed for acquiring facsimile transmission signals from telephone systems and converting these signals to a digital format. It then stores them onto a specially formatted DAT tape. The stored data can then be printed out at a central location for nothing with any of the other FAX MANAGER products. It is fully portable and housed in a rugged Hardside case. The unit is self-powered by a built in rechargeable battery, recharged by an AC adapter. The unit utilizes two working modes: 'send' and 'receive'. The send mode is used for the unattended recording of the facsimile signal. The manual mode is used for the playback of the signal, which can even be activated over the telephone line from a remote location to a central location where a STG FAX MANAGER is present."

SC
Hollywood, FL
Any, from what we hear, they're actually impossible to detect.
Prodigy Far From Gifted
Dear 2600:
I agree that Prodigy is a real turkey if only for its excessive advertisements, especially of users' mail, and remarkably slow response. (Oh yeah, and its demands for a loaded PC at times that few home users can afford. But STAGE-DAT really is the last straw. Contrary to the publicity given out by them when they claim that IBM and Sealed did intend to use home computers.
I'm sure of two things: First, if it is not in my role as a computer and private phone system technician, that proves this trick was done for and actually used for marketing purposes.
ONE: The STAGE-DAT file of one year was found to contain a whole group of mail addresses and telephone numbers when examined. Some of these did correspond to e-mail and numbers in other modem programs the person used, and some were in the same sub-directory path as Prodigy. There was a possible legitimate explanation.
The source of other names and numbers was a

mystery as they didn't correspond to names and numbers in my modem dialing list. The next soon found that they were in word processing files. But I'm sure that they were in word processing files. The version of word processing software I used (Microsoft's Wordstar) did not have a "release mode" (Prodigy had used word processing files in a different software).

As a rule, in rule out on incident of files that were once physically stored where Prodigy is now, whether was located and a secret within a company name with a phone number. That Prodigy was located, after this, STAGE-DAT was located in a file. The file name and number was found within a file. This proves that Prodigy deliberately incorporated this information very time it sent.

Two: In a place where I do living work, LANs are used with departments in 15th floors. If even has to be made with another work group (before LAN isn't gateway), it is done through networks, dialing through CompuLink.

Now, due to the software involved, these other locations are given greater routing address, numbers, and user name/alias domains, during names and connecting of a given of the location of family and Apple computers in given names are created. To support names like: APPLE LEGAL, BAKER LEGAL, CHARLEY LEGAL, DELTA LEGAL, ABLE SALES, BAKER SALES, CHARLEY SALES, DELTA SALES, ABLE SHIPPING, etc. are given to each computer.

Furthermore, these primary computer "names" are never used outside the company. Also, in the emergency, a person seeking a document to a certain computer in the legal department would know that it was in the legal department, but would not know the primary location given to that computer.

In short, there is no way, apart from reading the program, to know what arbitrary file names were given for system maintenance. And only management can read the password provided for

yet, shortly after installing Prodigy on several computers, just mail from Prodigy arrived in the company address in such "people" as ABLE SHIPPING, BAKER LEGAL, etc. showing that these names are assigned and actually used for marketing purposes.

While MSN (MSN) has a well-known flow that allows data to enter after it's been deleted, these two names in their phone call list is a serious. It really was a deliberate process. They just got caught.

Big Al
Brooklyn

A most interesting discovery. We think you should demand an explanation from the Prodigy people. If the company can show that this information was not intended to any way and used cover up with the proof that such names were generated, it should get away with it. It's the only way to determine what was intended. They were so quick to know what was happening here without doing a thorough investigation. We hope

more people continue to look into this and get answers that may do even more things.

General Questions

Dear 2600:

I enjoy reading your fine, informative magazine (although I have never read any of the interesting techniques described). There are a number of topics that I would like to have more information on and I was hoping that perhaps you might be able to help. These are my questions:

A. Temporal Java does a work? Is it a real threat? How can we shield our equipment? How can we use this technology in offensive roles?

B. Since direct dialing is restricted by the U.S. to many overseas countries, is there a way to bypass this problem? Is it possible to, for example, dial to a number in Canada where no one is home and, while the phone is ringing, use the 2600 area code to turn on the operator mode and enter the desired area code and number of the non-direct line country? Personally, I would be too afraid to turn on such a overage.

C. When you receive a busy signal after dialing a number, I have heard that it is possible to leave in the conversation by fast dialing a code not often including the number 3. Is this a common situation at this time?

D. Currently, New York State does not allow the phone company to offer ANI (Automatic Number Identification). Even though the state does not allow identification, I am curious as to how the state of the U.S. is possible to determine the answer of the incoming call prior to picking up the first set of digits after the introduction. I have heard of a code or key after what is sent with the ring signal? Also, is it possible to predict the security of your phone number when you're making a call, by perhaps entering some type of code?

E. Two years ago, I received a telephone call from a person about ten minutes after our transmission, my phone started to ring strange things. The phone rang with a very low, deep, muffled sound for about fifteen seconds. When I picked up the phone, no one was there. This happened several times over the course of the next half hour. Can you explain what was happening?

Wesley Longline
New York

A. What you're referring to are surveillance receivers that can read what is on a CRT screen in distance of up to a couple of miles. One such device is the TGR 2500 made by David Research in Sweden. Sweden (40 8 6700203). Temporal equipment is shielded against the fact of that, from of computer shielding, there are no real protection against the fact of that. You can take control in the fact that when you turn device on it probably be with more signal output during (AC) network and less CRDs. To the best of our knowledge, nobody else has been using such a device.

B. That kind of work has been used for quite some

line. It doesn't work so frequently anymore. But there's no reason why calls cannot be transferred legitimately to other numbers to go in different places. For instance, calls to Atlanta could be placed through C-Code before they were allowed from the Texas State. Candidates needing 600 numbers in the 710 area don't stop there, either. But it would be a great service if they could call a number in the 610 area and then transfer them to the 600 number they wanted. Such a service would be a great cost for the provider company.

C. Absolutely not.

D. What New York does is offer a Caller ID. ANI. However, it passed along to 600 number while the 710s just use whatever else. Anyone with an ANI number can go the number of the people calling them in the majority of cases. One way to protect your number from getting through is to go through an operator but we don't expect that method to last for long. In a way, it's better that so much attention is being paid to the C-Code ID issue when ANI just doesn't work without any questions being raised, and so for most people are concerned, they're just doing the same thing. In answer to your question, it is not likely that the Caller ID signal is being sent out since the service is not being offered. For that reason, you might be concerned as this point about your number being sent out through Caller ID. But you're not worried at ANI so you're safe.

E. For all we know, this happens every time a service calls, we'll just have to get around.

Red Box News

Dear 2600:

There's a Red Box somewhere nearby. Make sure the metal can of the new signal is not under any physical compression or stress when the speaker is repositioned. In my initial inspection it revealed to be identical operation (i.e., changes in the state of the code). The code should be made together without assistance in any way. I've noticed the speakers use slightly different (but structurally equivalent) sized components and sometimes it's difficult to get the new signal in. Just right without changing anything the two halves work together during the conversion. On one unit I ended up removing the unlabeled transducer near the speaker (it produces the high pitched beeps when in the programming mode) and measuring the signal with a small square of double-faced tape to the circuit board area where the transducer is just above. It's a good comforter placement if you can live without the programming beeps.

Also, in my area code (215), cellular telephones serviced by GTE Mobile only call me 600 area code. Could it be because they don't send out Caller ID information? I had a friend with a cellular phone call me on my Sprint 800 Line. I carefully noticed even the date and time of the call. When I received my phone bill and call detailing report, the

cellular call was listed there (I'm not saying that).

I tried the experiment a while later finding the phone ring five or six times before answering. This time my cell detailing showed the number 660-0012 and listed the city as Poplar Bluff, MO (a Christian suburb). This was a completely different number from my friend's cellular phone. When you call the number a recording begins the number and says "It is being checked for trouble." I've heard this recording for weeks now. It's interesting I got a phone number of all on the 600 bill. Can you figure out what the song is here?

Pete in Akron

In all likelihood, the number it was called by GTE Mobile which uses it as a phone company's only 600 number. ANI will not work then, you'll find a number why you get a recording when you're calling in. The "being checked for trouble" recording could mean anything, anything. It's not been said up for years.

Suggestions/Questions

Dear 2600:

I would consider myself a mid-level hacker, not a pre-adolescent. I remember the "old days" well, especially when thousands of my son were impossible to obtain. I remember the good old days of being stuck in the Midwest, and miss it terribly. I have a little experience working with Micro (from an Internet dialup, we had dialup to Micro), more experience messing with Internet (about 2-3 years and hacking), and various UNIX systems.

I've been a subscriber to PAP for a while, and even though the newsletter is distributed irregularly, I have the flavor of an underground publication. Please treat them with a little more respect, they're really good. After reading your publication, I'm and off for a number of years. I am disturbed by the administrative time you seem to be taking. Please, hire more people and get more personal.

RN

Later Forum, IL

We agree about PAP. But where the hell are they? We haven't seen a issue in weeks. Every advertisement is disappearing or not given word of it. It has to be a horrible deal now.

Dear 2600:

While reading some of your best issues, I noticed ads for 2600 Utilities and 2600 Linux Utilities. Are these all available? If so, how much? Also, do you know of any Internet Users' mode that you can sign up for? (I'm not sure that are available for emergency help).

Midnight Caller

You can try calling for help, instead of making whatever other suggestions. If PAP is for them, it should be for all. It's not a deal. The 2600 is a new short one and if we can get it together, other things will be better than.

Dear 2600:

I'm writing in regards to a company mentioned in the Station 91 issue, page 23 (International Microcomputer Corporation). I need a local phone number or address for the company because the 800 number listed in the article "The Two-Step" does not work in Canada.

RS

Saskatoon, Sask.

Canada

The address we have for that company is 3305 West 44th Avenue, Edmonton, Alberta T6C 2G4, Canada. We're not able to get a local number for you.

Dear 2600:

In a recent issue, you provided us with some 1 was wondering if anyone associated with 2600 would have access to or indexed disks of some of the recent MS-DOS "viral" viruses. In particular the Whistle Blower, Mother Fish, Swallow Virus, X The Whistle which was described in Pulpin 24 Hackin's Virus Information Summary List (February 14, 1991).

As you are so busy with your projects, I am not sure if you would be able to provide such a service. I am a student at the University of Alberta, and I am a member of the Whistle Blower Virus (February 14, 1991) and the Swallow Virus (February 14, 1991). I am a member of the Whistle Blower Virus (February 14, 1991) and the Swallow Virus (February 14, 1991).

These viruses, however, are about five years old and some of the most terrible viruses have more sophisticated and destructive capabilities (in fact, many of them have no "destructive" dimension, they simply attempt to avoid detection and reproduction). Although I am a student of programming, I find viruses and viruses are a useful means of learning "viral" code. I am a member of the Whistle Blower Virus (February 14, 1991) and the Swallow Virus (February 14, 1991).

Because of their relative immaturity, regardless of the ability, and interaction with their environment (operating systems and operating systems). It is somewhat surprising that in Dr. Decker's April 1991 special issue on Bacteriophages, there was no mention of viruses and viruses — only such "legitimate" programs as neural nets, genetic algorithms, and fractals. If you can provide me with further information or point me in the right direction I would appreciate it.

CS

Ottawa, Ontario

We suggest looking in the 2600 Microcomputer or page 41. If you're interested, it's available, but it's where it will end up.

Dear 2600:

My understanding is that there is a way to use your cellular phone to hear other phone calls when they're on. You need programs, not of course. This is supposed to work by entering a code into the phone's keypad, and then you can hear other cellular calls. I would like to try this out on my Microcellular telephone. I would be interested in seeing how it works on how this can be done.

SS

We suggest looking in the article "Cellular Phone Hacking" in the March 1991 issue of Microphone. Please if we get additional info on this kind of thing, we'll print it.

Caller ID Decoders

Dear 2600:

It is now possible to obtain free Caller ID decoder. Microsoft's Semiconductor, Inc. of Austin, TX has announced their new MIC-25497, a fully integrated, single-chip Caller ID decoder and ring detector. The semiconductor device can be integrated with LCD or LED displays, or a personal computer. The company is giving away free MIC-25497 sample kits with technical data to "qualified" electronic design engineers. Even the kit is free! The program to give your company name and application requirements. Microsoft can be reached at (800) 521-6376.

Build 5.

Hacking UNIX Passwords

Dear 2600:

In the last column, you asked and another later we've noticed the program called Thacker, published in the Spring 1991 issue because it was too easy to meet by system administrators. You both provided an alternative and a different way of hacking passwords. We got a copy of the published 300 and a copy of it. Mr. K. stated that you should get a copy of the program made for something that works like 10 from your target system, example 2, and use that on the target password. If you get all, you'll be a system with which means that it's built into the kernel. Therefore, there is no source code for it, unless you have the source code for the kernel itself, and anyone who says they have that is full of it. The only thing related to exploit that can be found in any directory or "viral" files will be the C language to the kernel's internal machine language routines, which is essentially worthless for achieving our desired goal here.

Basically, the encryption of passwords is unique to each system, which can be guessed by comparing the same encrypted password entry on two different systems. There are two different methods. There are two possible reasons for this: each version of UNIX uses its own proprietary encryption scheme, or by they all use the standard DES encryption algorithm, but they each use their own unique encryption seed. Either way, there is no way you can get at any of the information, since it is built into the kernel itself. Assuming the latter, even if you had the DES encryption source code, you wouldn't have the key, which could be any input sequence of random bytes, something which would be unobtainable.

If I had more, please tell me because I would have nothing more than to be able to easily implement what you guys are suggesting at home. As far as the only way to design passwords is to do it directly off of the

matrix system, which is, of course, very slick. Since your operating while monitoring the free exchange of information rather than watching a final line edit used, please explain how you would go about decrypting passwords or keys, since you believe that you can do it.

53

New Haven, CT

ENIGMA is a standard, meaning that it was designed to be the same for user and programmer as we would expect it to be. We are not sure that it also was a great deal more secure in writing and very convenient, depending upon the implementation, but the subject of a wide range of (OOPS) should be the same given the same input parameters. The key to the behavior of crypt() is the input parameters which consist of two strings or words of key. They are presented in strings so that we can remember and read them. The first parameter is the "password" as we all know it. The second one is the "salt," a string made up of two possibly random letters that is used as the seed to generate the encrypted password. Fortunately for the password keeper program, the encrypted password never with the same two letters as the salt, which gives us one of the two parameters to the crypt() procedure. The other one is the password itself, which is the key to the password file for a specific password might be different on a different system. If you create a new

password matrix, you are probably to obtain the same resulting encrypted password because the "salt" program usually refers to some mechanism to generate the "salt" after the successful login.

Finally, you should be able to implement the crypt() function at home, since the encryption algorithm is widely available.

Voice Mail Fun

Dear 2600:

I have discovered a neat little 1-800 voice mail system. It seems that 303.M.P.A.S. system handles all VMS messages to a centralized voice message bank. I have managed to find the voice bank number for British Petroleum (385 Australia). These numbers are listed as an added value.

The VMS requires an eight-digit username and up to 11 believed a 12-character password. Hence it's pretty hard to crack to get questions answered, so calling the voice bank and entering the extension of the person whose box you wish to access, the box opens. No username or password, no problem. You can delete, save, listen to, transfer, and reply in messages for free in the company.

NICK

Newcastle Upon Tyne
England

We can assure you that I don't work in any of the 303.M.P.A.S. systems or know. And it goes to show that things and differences can always pop up.

ridbits

You would think after all of the commotion about privacy invasion and lack of security that big corporations would begin to learn something. MCI can therefore be defined as learning disabled.

You may have seen the ads for their Friends and Family Circle gimmick. Basically, you get your friends and family to sign up for MCI. Then, whenever you call them (assuming you too have MCI), you can save on the regular rates. In a way, MCI has gotten their customers to do their selling for them. That part is actually rather clever. In fact, we've even heard of families putting the guilt trip on relatives who refuse to sign up with MCI.

But where MCI really messed up is with their 800 FRIENDS update service. This number exists so that customers can check the status of their calling circle — find out who's currently on it, who's been dropped, etc. The touch-tone service would ask you to key in your telephone number and then, to verify that it was really you, your zip code! Obviously, when you know somebody's phone number, figuring out their zip code isn't all that difficult. Yet this was the only bit of security standing in the way of anyone having access to customers' frequently dialed numbers. It made no difference if these numbers were unlisted. If they showed up on your calling circle, anybody could get them. And, not only that, but the relationship of the people in your circle was also announced. Example: "Your wife at 516-751-2600, your brother-in-law at 202-456-1414" and so on. One could get quite a bit of information on MCI customers rather quickly.

We had a bit of fun with this on WBAL's *Off The Hook*, the weekly telecommunications radio program in New York. We demonstrated the absurd security live on the air and told everybody to call MCI to complain. Apparently they did because the system was quickly changed. Now you need the last three digits of your second number for verification.

Those of you still mourning the loss of the various 800 ANI numbers can take comfort in a brand new number that's making the rounds. It's 208 an 800 number and we're told it doesn't charge. However the number won't work from payphones. It's 10732-404-988-9884. (You might have to dial a 1 before the 404.) It will only work with the 10732 carrier access code which is owned by AT&T. And for some reason, the recording seems to always add the number eight to the end.

It had to happen eventually. We finally found a 900 number that isn't a bad deal. For \$1.50, you can call 900-884-1212 and get a reverse listing on a phone number, assuming it's listed. Telephone of Springfield, VA has a database of over 80 million numbers and the human operators that answer don't try to keep you on for a long time. (If you do stay on, the cost is 75 cents a minute.) The only disadvantages are that numbers are only as updated as the next recent phone book from that region and the service is only called twice a week, on Friday. However, we hear that they will be automated before long.

There are many ways to send us letters. Our fax machine can be reached at 516-751-2608. Our Internet address is 2600@well.sf.ca.us. And for those of you who prefer the U.S. mail, our address is:

2600 Letters
PO Box 99
Middle Island, NY 11955

Letters may be edited for brevity or perhaps not printed at all. Anything is possible.

USPS HACKING

by The Devil's Advocate

The United States Post Office (USPS) is just like any other system. It is huge and complicated, with lots of acronyms and technical jargon. It is riddled with inconsistencies, and is prone to human error. Most importantly, it beckons to be explored by that very same bunch who are so fond of creative exploration: Hackers!

POSTNET

The Postal Numeric Encoding Technique (POSTNET) is a bar code system featured in 1983 to help accelerate the sorting of letter mail by automated equipment. The term "POSTNET" refers to a bar code

This POSTNET encodes 11953-0752.

119530752

where each digit represents either a five or a nine digit ZIP + 4 code. POSTNET is most often preprinted on business or courtesy reply mail by businesses. POSTNET can also be prepared on envelopes that are processed by an Optical Character Reader (OCR) machine.

POSTNET consists of a combination of 22 long bars and 30 short bars. The 52 bars encode a nine digit ZIP + 4 code plus a checksum number. Learning to read POSTNET is easy for anyone familiar with binary. The first and last bars (always long) are guide bars, and play no part in determining the encoded ZIP + 4. Each group of five bars after the first guide bar represents one ZIP + 4 number. The group consists of a combination of two long bars and three short bars. The position in the group has a corresponding value. The values from left to right are 7-4-2-1-0. A ZIP + 4 number is obtained by adding the values of the positions containing the two long bars. The only special case is when

the added values equal eleven. In this case, the number represented is zero. POSTNET also includes a checksum number at the end for the purpose of error detection. You can determine what the checksum number should be by adding the numbers of your ZIP + 4. The last digit of the resulting sum, when subtracted from 10, will yield the checksum number. For instance, if your ZIP + 4 is 11953-0752, then the sum is $1+1+9+5+3+0+7+5+2=33$, the last digit of the sum is 3, and the checksum is $10-3=7$.

The USPS encourages companies to preprint the ZIP + 4 POSTNET on reply mail by affixing a postage meter. The advantage of using POSTNET is not only in savings but in speed. Letter mail that uses POSTNET is processed faster and more accurately than mail which does not use POSTNET.

MARK

The MARK face character serves three purposes: 1) It cancels and postmarks letter mail; 2) It arranges letters so that they all face in the same direction; 3) It separates POSTNET letter mail from mail that does not use POSTNET.

The MARK utilizes fluorescent and phosphorescent detectors that enable it to detect the presence of minute traces of phosphor on stamps, pre-stamped postcards or envelopes, and meter marks. The MARK is also capable of detecting preprinted Facing Identification Marks (FIM).

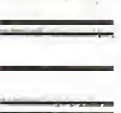
FIM

Open any magazine and you will find business reply mail cards inside. Nearly every card will contain a FIM. These six-

line bar codes are much better than POSTNET, but not nearly as wide. They are located at the top of the card, just left of the postage area. The MARK recognizes four types of FIMs:

FIM A

Letter uses POSTNET, and needs postage. Used for courtesy reply mail.



FIM B

Letter does not use POSTNET, and does not need postage. Used for business reply mail.



FIM C

Letter uses POSTNET, and does not need postage. Used for business reply mail.



FIM D

Letter does not use POSTNET, needs postage, and is OCR readable. Used for courtesy reply window envelopes.



The MARK first checks to see that a letter has postage (stamp, meter mark, or FIM). After passing this test, the letter is then cancelled, postmarked, and directed to one of eight bins based upon the orientation of the letter and the presence of POSTNET. Four of the eight bins are for POSTNET letter mail, while the other four bins are for mail that does not use POSTNET. Each group of four bins accepts letters according to their orientation. Because letters can enter the

machine right side up, upside down, backwards, or forwards, the MARK must have a bin for every possible orientation. The MARK also utilizes a ninth bin for letters that are rejected by the machine for lack of postage. For example, if a letter does not have postage, and the letter does not have FIM B or FIM C (indicating that no postage is necessary), then the letter will end up in the reject bin. Sometimes letters that do have legitimate postage may end up in the reject bin. If a stamp is not placed in the upper right hand corner of an envelope, then the MARK's sensors may not detect the phosphor, and the letter will be rejected. A clerk manually goes over all of the rejected letters individually to determine why they were not processed.

LSM

The Letter Sorting Machine (LSM) was first used by the USPS in the late 1950's. The huge semi-automatic beast requires a group of operators to sit in front of twelve consoles while letters are flipping by at a rate of one foot second. The machine automatically positions a letter in front of an operator, who then has one second to key in the last three digits of the ZIP code. The letter is then whisked away to one of several hundred bins according to the keys that were depressed. If an operator fails to key in anything then the letter will go to a reject bin and will eventually be fed back into the LSM. If an operator happens to key in the wrong



code, then a slight possibility exists that the misprinted letter will be caught by a clerk before it is shipped. Otherwise, the letter will be delivered to that location, wherever it may be, and will eventually be delivered back again.

LSM places a marker on the back of every letter that is processed. The marker consists of two alphanumeric symbols. The first symbol is always a letter ranging from A to Z. The second symbol is either a letter ranging from A to C, or a number ranging from 1 to 9. The marker can therefore be one of 319 possibilities. The marker may also be one of several different colors, although the color does not indicate any useful information. According to USPS LSM operators, the marker indicates which console processed the letter. However, this information is fairly useless because we still do not know which specific LSM processed the letter. The USPS uses hundreds of LSMs nationwide, and each of these LSMs has twelve consoles. I am uncertain how to translate a specific marker into a specific console, nor do I understand why the marker can be one of 319 possibilities if there are only twelve consoles.

BCS

The Bar Code Sorter (BCS) processes POSTNET letter mail. The BCS is therefore limited to sorting only business reply mail and other high volume mail which incorporates the POSTNET. At a sorting rate of ten letters per second, the BCS is considered slightly faster than your average clerk. The letters must be properly positioned and fed into the machine manually by an operator. This is accomplished by stacking trays of letters received from the MARK into a feeder unit. The operator does not have to properly position each letter because the letters received from the MARK are already facing the same way.

MLOCR

The Multiline Optical Character Reader (MLOCR) is the latest and most advanced machine in the USPS letter sorting arsenal. This million-dollar monster is capable of reading all of the lines that comprise a letter's address. It then takes this information and compares it against its own internally stored address directory. Finally, an appropriate POSTNET is set sprayed on the letter so that it can be further processed by a BCS. The purpose of the MLOCR is therefore to spray POSTNET on letters that do not use POSTNET, so that they can be processed by a BCS.

The advantage of the MLOCR is that it can determine an address even if parts of the address are illegible, incorrect, or missing. For instance, if someone forgets to include a ZIP code, or uses the wrong ZIP code by mistake, then the MLOCR can still determine the correct ZIP code by comparing the street, city, and state with its own address directory. It will then spray the letter with the correct ZIP + 4 code (the MLOCR will always try to spray the letter with a ZIP + 4, even if the letter uses a five digit ZIP code).

Clearly OOCRs could only read type or clearly printed handwriting. In the near future, however, the MLOCR will recognize script as well. The MLOCR is capable of reading the address even if it is skewed (i.e. printed at an angle). The MLOCR does not have the capability of knowing whether or not a letter already has POSTNET, nor can it sort mail according to POSTNET. Therefore, it is possible to receive a letter that has two overlapping POSTNET bar codes.

Like the BCS, the MLOCR only accepts trays of properly positioned machineable letters that must be fed into the machine manually by an operator.

Mail Hacks

There are at least three things that everyone familiar with the USPS would

like to do: 1) Mail letters for free. 2) Get their letters delivered quicker. 3) Find out why it takes so long for their letters to arrive.

Free Mail

It is not difficult for someone to mail a letter for free. It is, however, extremely difficult to mail many letters for free. The USPS is always looking out for mail fraud, and has an entire agency devoted to just this task. Even if a good mail hack works once, it is not likely to work if used repeatedly. Therefore, if you are reading this article with the intent of saving money by tricking the USPS and mailing letters for free, then you would do better to give up now before you are busted. Of course, anyone with even the slightest iota of curiosity would want to know some of the methods.

Perhaps one of the oldest seams in the book is to switch the destination address with the return address and mail the letter without postage. The USPS will then return the letter to its "sender" for postage. Of course, the USPS is not that stupid, and this trick rarely works for nonpaid mail.

A much better mail hack would be to use a laser printer to print a FIM B on an envelope. The MARK will then treat the letter like a business reply mail card, and will not reject it for lack of postage. Of course, the problem with this technique is that a mail carrier will almost certainly notice the missing postage before the letter even gets to a MARK. Therefore, you would have to bundle this letter with another letter that has postage, place the letter with postage on top of the illegitimate letter, and use a rubber band to bundle them together. The mail carrier will not disturb this bundle. Eventually, the bundle will reach a General Mail facility (GMF) where clerks quickly separate bundles on a conveyor belt. It is extremely unlikely that they will notice the illegitimate letter at this point. From the

conveyor belt, the letter will journey to the MARK. Once the MARK processes the letter, it is unlikely that anyone will notice the missing postage until the letter reaches its destination. The final obstacle is the mail carrier that will physically deliver the letter to its destination. At this point, the letter is postmarked, so one can only hope that the mail carrier is not too nosy.

Fast Mail

Getting your letters mailed quickly is a much better hack than trying to mail your letters for free. Not only is it legal but the results are guaranteed.

Normally, a letter reaches a MARK where it is processed and sent to an MLOCR. If the address on the envelope is readable by the MLOCR, then it is just sprayed with a POSTNET and sent to a BCS. Otherwise, the letter is rejected and sent to an LSM. The one thing you really want to avoid is having your letter processed by an LSM. The operators who run these machines are notorious for keying in the wrong code, causing your letter to journey out of its way to strange and exotic parts of the country. Never write the address on your envelope in script unless you want to delay your letter.

One way you can get your letters processed quicker is to have your letters skip some of the steps in the sorting process. The method involves using a laser printer to print a FIM A and a POSTNET on an envelope. The FIM A will instruct the MARK to treat the envelope as courtesy reply mail. The MARK will look for postage, which you have thoughtfully provided, and then send the letter into a bin with all of the other POSTNET mail. This mail will then be placed in a tray and sent directly to a BCS, skipping the MLOCR and completely avoiding the LSM.

By using POSTNET, you are taking advantage of the same multilink dollar equipment that is used by businesses.

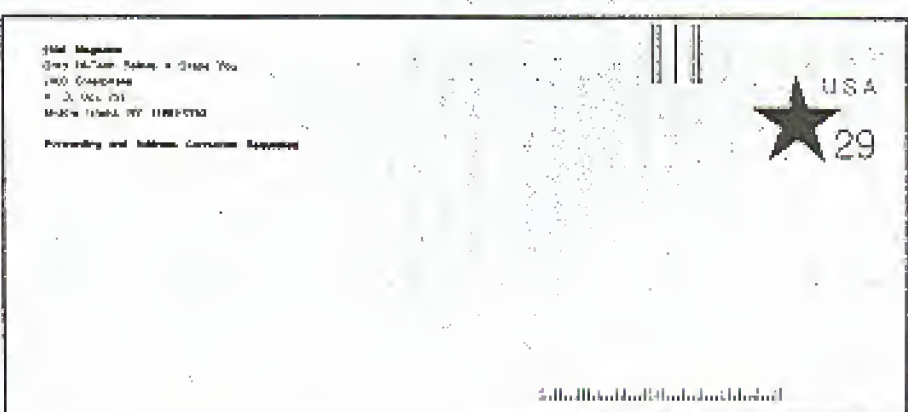
Marketing Department
Regular Mail Services Division
U.S. Postal Service Headquarters
475 L'Enfant Plaza SW, Room 354
Washington D.C., 20560-6336

Sunni Shi'ite

Now that you know what happens to your letter when you mail it, you can use this information to determine why it takes so long for your own mail to arrive. The next time a letter comes in the mail, analyze it for reliable USPS markings that may give you insight into how the letter was processed. If the letter has POSTNET on it, then you know that the letter was processed by an M/CCK and a BCS. You can then read the POSTNET to make sure that it represents your ZIP code. If there's no POSTNET is incorrect then that would certainly explain why your letter was delayed. You should also flip the letter over and look for LSI markers. You should not see any more than one or two markings. If the back of your letter is covered with them, then you know that your letter probably had quite a journey whipping back and forth around the country before it reached you. Keep in mind that it is not unusual for a letter to be processed by both a BSC and an LSI. Not all GMFs use the same machinery, and the average clock can screw up any letter, even if it is processed by machines.

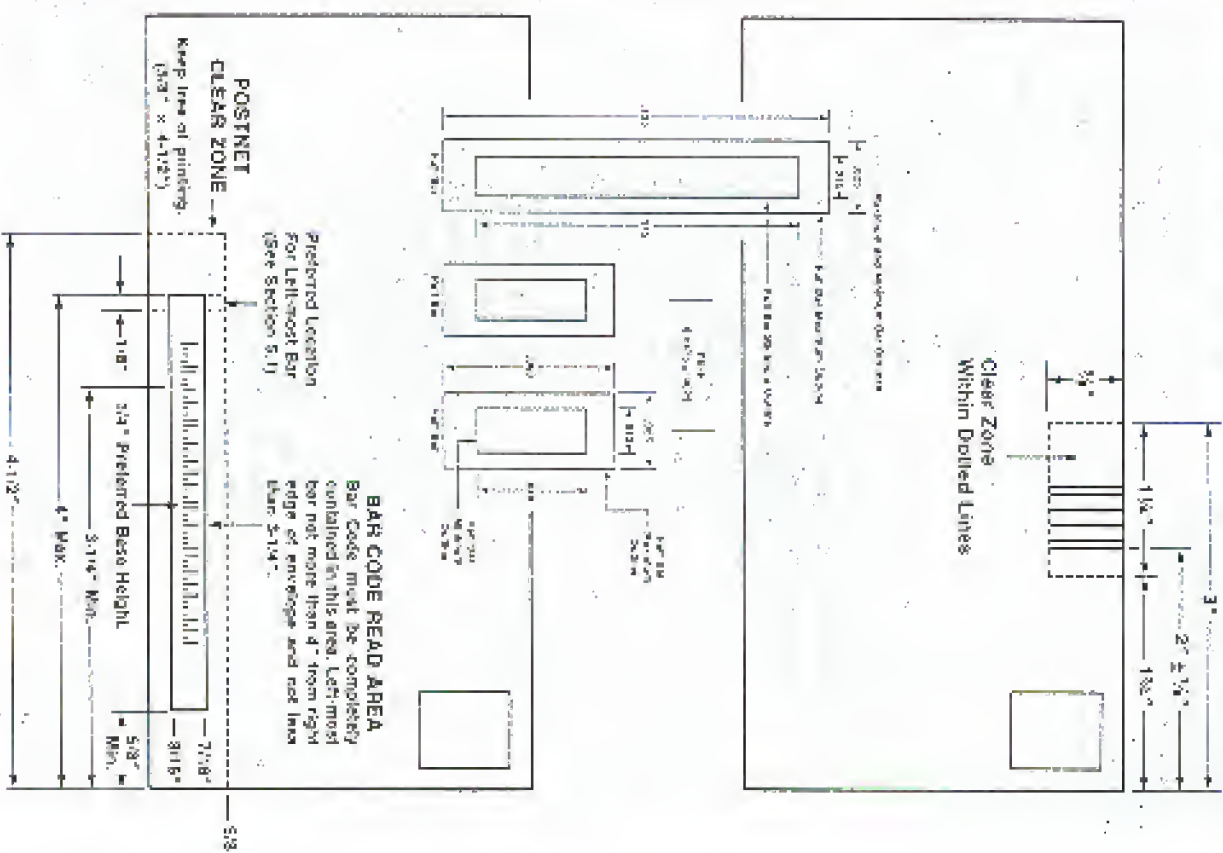
Further Reading

For those of you who are interested in learning more about XOSNET and the machines that process mail, we suggest that you obtain a *Guide to Business Mail Preparation*. The pamphlet is produced by the USPS (Publication 23) and is available free-of-charge to all business customers. You can request a copy through the mail by writing to this address:



We designed the FIM A and the POSTNET on this envelope using a standard desktop publishing software. A laser printer was used to print the two barcodes on the pre-stamped envelope. If we ever decide to mail this letter, it should get back to us with all the speed afforded to courtesy reply mail.

This information was obtained from *A Guide to Business Mail Preparation* (Publication 25). Use these diagrams to design your own FIM and POSTNET.



PSYCHOLOGY IN THE HACKER WORLD

by Condor Woodstein

We are all descended from a successful tribe of 15 to 80 hunter-gatherers, so it is no surprise that we fall into categories. Mythologists call them archetypes: the Orphan, the Warrior, the Wanderer, and so on. The Enforcer is an archetype, a genetic personality type that exists in every society.

At its most extreme, the enforcement personality is a paranoid schizophrenic, unable to distinguish friend from foe. In America, these types are (ideally) ferreted out by Internal Investigations. In other places, these crazies rule the nation.

First and foremost, Enforcers are convinced of the rightness of their ideas. Philosophical doubts are useless. If the legislature were to make hard-boiled eggs illegal, Enforcers would pursue people who sell and consume hard-boiled eggs with the same vigor now devoted to hackers. In this sense, the Enforcer actually shows an amazing elasticity of belief. The mere passage of a bill into law will re-organize the thinking of the Enforcer.

As a corollary, the Enforcer is incapable of learning from experience. No matter how often a belief is proved wrong by physical evidence, the Enforcer claims that better equipment or tougher laws will solve the problem.

William J. Cook is the federal prosecutor who busted Shadowhawk and who stepped the presses at *Phrack*. He told the tale of how he nailed Shadowhawk in a magazine

called *Security Management*. Reading this periodical provides an insight into the mental mechanisms of the Enforcer.

"Uncovering the Mystery of Shadowhawk," by William J. Cook appeared in the May 1990 issue. Cook explains how the hacker got into NATO, Air Force, and AT&T computers and then says, "Shadowhawk's method of operation was based less on genius and more on using passwords, user tips, and hacking techniques learned from hacker bulletin boards."

The above is an example of *denial of genius*. As a programmer, you know that other programmers do things well that you do not and vice versa. You have no problem admitting that someone else is smarter than you. This is impossible for the Enforcer. It is easy to take Cook's statement and make it into a Nazi refutation of Relativity: "Einstein's theories are based less on genius and more on Newton's calculus. Maxwell's physics, and tensor algebra, learned from other mathematicians."

"Doing Time on the Telephone Line," by Langford Andersen was published in the February 1990 issue of *Security Management*. Andersen is the communications director of The Communications Fraud Control Association in McLean, Virginia. In outlining the many ways that telephone companies are cheated out of their revenues, he explains the "code calling" fraud, perpetrated on AT&T by trucking companies. "The caller

would ask the operator to place a collect call for Fred P. Jones III. The call would be refused, but the name was a code that let the company know a driver has left a load in Nashville en route to Kansas City. This would go on 24 hours a day, seven days a week, and the cost in AT&T operator time was incredible."

This is an example of *denial of opportunity*. AT&T defined its own system. Yet by taking advantage of that system, these trucking companies committed "fraud" in the eyes of the Enforcer.

It is also an example of *tunnel vision*. Trucking companies were not the only ones who benefited from this insight. Salesmen calling home, college kids, millions of people took advantage of this loophole in AT&T policies. The fact that AT&T survived suggests that these costs were already built into the phone rates. Perhaps we are to believe that this activity kept into sudden existence in 1970 and only discontinue saved the company.

Yet another example of this *tunnel vision* comes from Brian D. Costley's "Cracking Down on the New Safe-cracker." No, it isn't a reincarnation of Richard P. Feynman, it's an autodialer that can spin 280,000 combinations in 30 hours. The article surrounds an ad for combination locks by Sargent and Greenleaf, the company that employs Costley. This blatant example of feathering one's own nest is lost on the Enforcer who passively accepts the offerings of any authority figure. Simple arithmetic would indicate that the S&G dual-dial combination locks are only a bigger, not impenetrable, barrier. It is almost humorous that the S&G ad

relies on registered trademark phrases: "spy-proof" and "manipulation-proof." (Think of how cool it would be to nail a sign to your home that says "Winston Castle (TM).")

Despite the image of the Enforcer who is dedicated to facts (promulgated by police procedural mysteries), the truth is that at some point, the belief structures of the enforcer can only be protected by vagueness.

An example of this *denial of objective reality* can be found in "Defending Against Virus Attacks," by Raymond G. Kummer, the deputy director of the National Institute of Standards and Technology. The article appeared in the May 1990 issue of *Security Management*.

How does one defend against viruses? No answer is given. The article alludes to private sector solutions, but none is named. The article describes committees, studies, and news releases. In response to the Internet Worm (the calls it a "virus"), the NIST worked with the Department of Defense and the National Security Agency. Rather than create computer programs they created another committee which in turn warned computerists about the Columbus Day Virus of 1989 but failed to provide any products.

For many Enforcers, this divorce from reality eventually manifests itself as paranoia. A perfect example of the denial mechanisms involved comes from "Headache for the Host" by Darlene M. Tester, *Security Management*, January 1990. The article is a complaint against "a new protocol in data processing — the transfer from PC to host." The author also says, "A chorn in the side of the software industry has been

public domain software.... In the past, these software packages have been available through PC network bulletin boards and pirate data reproduction services.... File transfer protocols are entering this sector of the software industry.... Unlike other public domain packages, this software comes under the guise of a different name — "nonpublic domain software."

Tester's solutions to the threat of file transfer protocols are to forbid users from mounting such software. Feeling that, if users are actually permitted to load programs, then the system administrator must "print a hardcopy of the protocol and review it for logic bombs or time bombs." If she can read hex code that well, I admit she is smarter than I'll ever be.

Projection and transference are psychological mechanisms that manifest themselves strongly in neurotic individuals. Tester uses the phrase "foirly tale existence" and accuses unnamed persons of individuals.

claiming that unnamed security people are "paranoid."

Continuing not to name names, Tester alludes to "name-brand protocol systems" that are safe and reliable, but doesn't name any. Tester closes her article with the paranoid's manifesto: "Fast systems have a good safety record. That safety record must be maintained at all costs." Would Tester draw the

line at executing one Diskmo in ten if it meant that mainframes would be safe from viruses? You can gauge the level of reality denial by considering that, as a woman, Tester is a "host." She fears "mounting," "penetration," and "infection" and in fact, "has a headache." If she would face these fears, they wouldn't appear in her technical essays.

You can see from these examples that the Enforcer is a terrible servant and a fearful master. Only the strongest judicial and constitutional restraints will protect America from these deluded individuals.

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

2600 marketplace

2600 MEETINGS: First Friday of the month at the Chicago Center from 5 to 8 pm in the lobby near the payphone, 133 E 53rd St., N.Y. between 1st & 2nd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Chicago: 212-225-4011, 212-221-8927, 212-308-8024, 212-308-8182. Meetings also take place in San Francisco at 4 Embarcadero Plaza (outside) starting at 5 pm. People Time on the first Friday of the month. Payphone numbers: 415-398-9809, 415-36.

WANTED: Schematics and data bits for telephone line voice scramblers. Prefer digital tools using DES unencrypt-encrypt algorithm. Tools may be used cheaply from elevator of unit. Please send photocopies to A.G. Morris, PO Box 4821, Long Beach, CA 90804-4821.

SPY SHOP CATALOGUE: Packed with equipment, maps, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, scan guns, room monitors, decoding devices, analyzers, covert tracking systems, detector systems, seller ID, people tracer - find anyone anywhere! Detection systems, tap vops, voice changes, scanners, secure phones, and much more. Send \$5 check or money order to: Bug Busters, PO Box 578, Dept. 2A, Shorttem, NY 11786. FAX 516-929-0772.

WILEY PAYS \$14,000 for "trained radio" computer program and software. Call Mike at 212-533-4331.

KNOW WHO'S CALLING? The Call Identifier has the answer. Displays caller's phone number when your phone rings. Shows phone numbers with date and time of call. \$79.95. \$10 off for 2600 subscribers. Surveillance Counterintelligence equipment available \$5. Miniature Surveillance Transmitter Kit, \$39.95 p/d. Voice changers, scramblers, vehicle tracking, bug and phone tap detectors, books, videos, etc. J.D.E., PO Box 337, Buffalo, NY 14226. (716) 691-3436.

CAN SUPPLY software and computer hardware of any kind below wholesale prices. I am looking for sales people. If you can find me buyers, I will work out a percentage. Would like to correspond with hackers in Switzerland, Germany, Japan, and France. Anybody with access to wealth transfer methodology or access to

Los Alamos National Laboratory in New Mexico and/or Lawrence Livermore Labs in San Francisco. K. Henderson, PO Box 265, Aurora, IL 61301. 818-859-6351.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES: The first book on how to write them! 199 pgs, soft cover, with full IBM PC source code \$14.95 postpaid, or ask your local bookstore to order it. ISBN 0-929408-02-0. American Eagle Publications, Box 6146, Tucson, AZ 85710.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Bass Engineering, Inc., 7904 Hope Valley Court, Adamstown, MD 21101. 800-435-3280.

COCOTS FOR SALE: Perfect working condition, removed from service. Cash and only type, has and reader built into unit. 1715E, 12 number speed dial, \$89 each plus \$15 shipping. Call or write for info. Bill Rogers, 2010 E. Charlotte Blvd., Las Vegas, NV 89106. 800-669-8506. (702) 352-7348.

TAP BACK ISSUES, complete set (as 1, 91, high quality, \$50. SASF for info, info on other holdings. Robert H., 1209 N 70th, Wapato, WA 99173.

TAP BACK ISSUES, complete set Vol 1-9 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid. Via UPS or First Class Mail. Copy of 1973 Equine article "The Secrets of the Little Blue Box" \$5 & large SASF web2 suite of stamps. Pete G., PO Box 453, Mt. Laurel, NJ 08054. We are the Original!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 1/15/92.

MORE EXCITING PRISON NEWS

PUBLICATION CENSAL NOTIFICATION

TITLE OF PUBLICATION 2600 Magazine Quarterly, Spring 1991, Vol. 11

The above publication has been reviewed and identified in accordance with Section 3.9 of the TDCJ Rules and Regulations for the reasons checked below.

- ☐ (a) Publication contains prohibited explosives, weapons or drugs.
- ☐ (b) Publication contains information regarding the manufacture or distribution of weapons or drugs.
- ☐ (c) Publication contains material that a reasonable person would constitute as written advice for the purpose of communicating information designed to achieve a breakdown of prisons through inmate disruption such as strikes or riots.
- ☐ (d) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviate criminal sexual behavior.
- ☐ (e) Publication contains material on the selling up and operation of criminal schemes or how to avoid detection of criminal schemes by law enforcement charged with the responsibility for detecting such illegal activity.

REMARKS: Pages 1, 3, 4, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 98, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Institutional Division, within two (2) weeks of the date shown below.

MAIL SYSTEM CORRESPONDENCE PANEL

October 9, 1991

DATE

2600 Magazine
Palmer, Sender
P.O. Box 752
Address
Huntsville, TX 77340-0752
City, State, Zip Code

Our magazine has been called just about everything under the sun, but this is a new one on us.

more conversion tricks

by DC

The Radio Shack red box conversion is the greatest example of a remarkable coincidence that I have ever come across. The fact that the tuning of the microprocessor inside the device and the same pair for the DTMF asterisk when speed up creates a nearly perfect quarter tone sequence is beyond luck. The entire conversion is poetry. Thanks for the great work, Neath Clayton.

Being that the tone dialer itself is such a nice product (I believe it is, feature for feature, the best product Radio Shack has to offer, considering most of what Radio Shack has to offer socks and its overpriced anyway) I didn't want to just convert it into a red box. I wanted to have the red box serve as well as the dialer capabilities.

Since reading the conversion article in the Autumn 1990 issue of 2600, I have come across a file explaining how to make the conversion but incorporating a switch to select between the two different frequency crystals, enabling both touch tones and a red box. One thing I didn't like about the file's design is that it had wires coming out of the back of the unit on the two crystals and the switch which were all exposed together to the back of the unit.

Ugly. I managed to fit everything neatly inside the unit.

The first thing I did was file the lip on the bottom of the 6.5536 Mhz crystal flush with the rest of its case to give it a lower profile. Looking at the circuit board with the battery compartment towards you, I removed the screw on the upper left-hand side near the two solder pads and diode and put the crystal in that area. I also reduced the solder on the lower pad to make the slightest bit more room for the crystal. I soldered one lead of the 6.5536

Mhz crystal (extended with a piece of wire) to one lead of the 3.579545 Mhz crystal. I then soldered the other lead to the top leg of the SPDT switch and glued the crystal in place with some super glue. I then desoldered the other leg of the 3.579545 Mhz crystal and jumpered it to the bottom leg of the SPDT switch. Finally, I soldered a jumper from the middle leg of the switch to the lead into the microprocessor (the lead that one leg of the 3.579545 Mhz crystal was desoldered from). I cut a slot in the side of the two halves of the case (the side opposite the ON/OFF and DIAL/STORE switches) and glued the switch in place. It works like a charm.

The 6.5536 Mhz crystal can also be ordered from Radio Shack by the way, for \$4.95 each. I wouldn't mention this if it weren't for the fact that Fry's Electronics wanted to charge me eight bucks shipping and handling alone on a cash order.

I also discovered that the tone dialer can be converted to generate the green box "coin return" tone. Repeating the 3.579545 Mhz crystal with one that has a value close to 4.1931 Mhz (the calculated value) will cause the pound (4) key to generate frequencies close enough to the 1100 and 1700 Hz green box tones (1091 and 1713 to actually). Making this mod to the dialer wouldn't suffice because you would still need a way to generate either 2600 Hz or 900-1500 Hz (the "operator release" signal) in order to send the green box tones. If someone can figure out how to incorporate all needed green box tones into the dialer, I would like to hear about it. It would be a nice complement to the red box.

Readers, Please send us your experiences and experiments to share.

| | | | | | | |
|--------------|----------|-------------|-------------|-------------|-------------|-------------|
| 43 (15) 2 | 524 (13) | 231 (45) | (23) 1 (45) | (123) 54 | (123) 54 | 24 (135) |
| 14 (23) 5 | 542 (13) | 312 (45) | (24) 5 (13) | (124) 35 | (124) 35 | 42 (135) |
| 15 (23) 4 | 235 (14) | 321 (45) | (24) 3 (15) | (124) 53 | (124) 53 | 23 (145) |
| 41 (23) 5 | 253 (14) | (12) (34) 5 | (24) 1 (35) | (125) 34 | (125) 34 | 32 (145) |
| 45 (23) 1 | 325 (14) | (12) (35) 4 | (25) 4 (13) | (125) 43 | (125) 43 | 15 (234) |
| 51 (23) 4 | 352 (14) | (12) (45) 3 | (25) 3 (14) | (134) 25 | (134) 25 | 51 (234) |
| 54 (23) 1 | 523 (14) | (13) (24) 5 | (25) 1 (34) | (134) 52 | (134) 52 | 14 (235) |
| 13 (24) 5 | 532 (14) | (13) (25) 4 | (34) 5 (12) | (135) 24 | (135) 24 | 41 (235) |
| 15 (24) 3 | 234 (15) | (13) (45) 2 | (34) 2 (15) | (135) 42 | (135) 42 | 13 (245) |
| 31 (24) 5 | 243 (15) | (14) (23) 5 | (34) 1 (25) | (145) 23 | (145) 23 | 31 (245) |
| 35 (24) 1 | 324 (15) | (14) (23) 3 | (35) 4 (12) | (145) 32 | (145) 32 | 12 (245) |
| 51 (24) 3 | 342 (15) | (14) (35) 2 | (35) 2 (14) | (234) 51 | (234) 51 | 21 (245) |
| 53 (24) 1 | 423 (15) | (15) (23) 4 | (35) 1 (24) | (234) 15 | (234) 15 | (123) (45) |
| 13 (25) 4 | 432 (15) | (15) (24) 3 | (45) 3 (12) | (235) 14 | (235) 14 | (124) (35) |
| 14 (25) 3 | 145 (23) | (15) (34) 2 | (45) 2 (13) | (235) 41 | (235) 41 | (125) (34) |
| 31 (25) 4 | 154 (23) | (23) (14) 5 | (45) 1 (23) | (245) 13 | (245) 13 | (134) (25) |
| 34 (25) 1 | 415 (23) | (23) (15) 4 | 3 (12) (45) | (245) 31 | (245) 31 | (135) (24) |
| 41 (25) 3 | 451 (23) | (23) (45) 1 | 4 (12) (35) | (345) 12 | (345) 12 | (145) (23) |
| 43 (25) 1 | 514 (23) | (24) (13) 5 | 5 (12) (34) | (345) 21 | (345) 21 | (234) (15) |
| 12 (34) 5 | 541 (23) | (24) (15) 3 | 2 (13) (45) | 4 (123) 5 | (235) (14) | (235) (13) |
| 15 (34) 2 | 135 (24) | (24) (35) 1 | 4 (13) (25) | 5 (123) 4 | (245) (11) | (245) (11) |
| 21 (34) 5 | 153 (24) | (25) (13) 4 | 5 (13) (24) | 3 (124) 5 | (345) (12) | (45) (123) |
| 25 (34) 1 | 315 (24) | (25) (14) 3 | 2 (14) (35) | 5 (124) 3 | (45) (123) | (35) (124) |
| 51 (34) 2 | 351 (24) | (25) (34) 1 | 3 (14) (25) | 3 (125) 4 | (35) (124) | (35) (124) |
| 52 (34) 1 | 513 (24) | (34) (12) 5 | 5 (14) (23) | 4 (125) 3 | (34) (125) | (34) (125) |
| 12 (35) 4 | 531 (24) | (34) (15) 2 | 2 (15) (34) | 2 (134) 5 | (25) (134) | (25) (134) |
| 14 (35) 2 | 134 (25) | (34) (25) 1 | 3 (15) (24) | 3 (134) 2 | (24) (135) | (24) (135) |
| 21 (35) 4 | 143 (25) | (35) (12) 4 | 4 (15) (23) | 2 (135) 4 | (23) (145) | (23) (145) |
| 24 (35) 1 | 314 (25) | (35) (14) 2 | 1 (23) (45) | 4 (135) 2 | (15) (234) | (15) (234) |
| 41 (35) 2 | 341 (25) | (35) (24) 1 | 4 (23) (15) | 2 (145) 3 | (14) (235) | (14) (235) |
| 42 (35) 1 | 413 (25) | (45) (12) 3 | 5 (23) (14) | 3 (145) 2 | (11) (345) | (11) (345) |
| 13 (45) 2 | 431 (25) | (45) (13) 2 | 1 (24) (35) | 1 (234) 5 | (12) (345) | (12) (345) |
| 12 (45) 3 | 125 (34) | (45) (23) 1 | 3 (24) (15) | 5 (234) 1 | (1234) 5 | (1234) 5 |
| 21 (45) 3 | 152 (34) | (12) 5 (34) | 5 (24) (13) | 1 (235) 4 | (1235) 4 | (1235) 4 |
| 23 (45) 1 | 215 (34) | (12) 4 (35) | 1 (25) (34) | 4 (235) 1 | (1245) 3 | (1245) 3 |
| 31 (45) 2 | 251 (34) | (12) 3 (45) | 3 (25) (14) | 1 (245) 3 | (1345) 2 | (1345) 2 |
| 32 (45) 1 | 512 (34) | (13) 5 (24) | 4 (25) (13) | 3 (245) 1 | (12345) 1 | (12345) 1 |
| 34 (45) (12) | 521 (34) | (13) 4 (25) | 1 (34) (25) | 1 (345) 2 | 5 (1234) | 5 (1234) |
| 35 (45) (12) | 142 (35) | (13) 2 (45) | 2 (34) (15) | 2 (345) 1 | 4 (1235) | 4 (1235) |
| 43 (45) (12) | 214 (35) | (14) 5 (23) | 5 (34) (12) | 4 (5) (123) | 3 (1245) | 3 (1245) |
| 45 (45) (12) | 241 (35) | (14) 3 (25) | 1 (35) (24) | 5 (4) (123) | 2 (1345) | 2 (1345) |
| 53 (45) (12) | 412 (35) | (15) 4 (23) | 4 (35) (14) | 3 (5) (124) | 1 (2345) | 1 (2345) |
| 54 (45) (12) | 421 (35) | (15) 3 (24) | 1 (45) (23) | 3 (4) (125) | 3 (4) (125) | 3 (4) (125) |
| 25 (45) (13) | 123 (45) | (15) 2 (34) | 2 (45) (13) | 4 (3) (125) | 2 (5) (134) | 2 (5) (134) |
| 42 (5) (13) | 132 (45) | (23) 5 (14) | 3 (45) (12) | 2 (5) (134) | 5 (2) (134) | 5 (2) (134) |
| 45 (2) (13) | 213 (45) | (23) 4 (15) | (123) 4 5 | | | |



TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER

PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF

REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN

BOUNDED OUR (FOREFEEL) READERS. SO YOU COULD FIND

YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN

THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS

HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE

TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE

EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT

ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR

LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS.

RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO

WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU

CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO

PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME

SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY

OF THIS AGAIN.



INDIVIDUAL SUBSCRIPTION

☐ 1 year/\$21 ☐ 2 years/\$38 ☐ 3 years/\$54

CORPORATE SUBSCRIPTION

☐ 1 year/\$50 ☐ 2 years/\$90 ☐ 3 years/\$125

OVERSEAS SUBSCRIPTION

☐ 1 year, individual/\$30 ☐ 1 year, corporate/\$65

LIFETIME SUBSCRIPTION

☐ \$260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

☐ 1984/\$25 ☐ 1985/\$25 ☐ 1986/\$25 ☐ 1987/\$25

☐ 1988/\$25 ☐ 1989/\$25 ☐ 1990/\$25

(OVERSEAS: ADD \$5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988, 1989, 1990 are \$5.25 each)

TOTAL AMOUNT ENCLOSED: